REMARKS

Claims 1-5, 7-13, and 15-34 were pending in the application, with Claims 1, 9, 16, 23, and 30 being independent. Applicant amends Claims 1, 9, 16, and 23-30 to further clarify features of the claimed subject matter. The original specification and drawings support these claim amendments at least at pages 4-9, and in Figures 1 and 2. These revisions introduce no new matter.

Claims 1-5, 7-13, and 15-34 are now pending in the application. Applicant respectfully requests reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks.

Claims Rejections Under 35 U.S.C. § 101

Claims 23-29 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Applicant amends independent Claim 23 to recite in pertinent part, "*A method for running a protocol for establishing a trust relationship between two or more processing nodes, comprising*". Applicant also amends dependent Claims 24-29 in a similar manner. The support for these amendments may be found in the original specification at least on pages 7-9, thus no new matter has been introduced.

As discussed during the telephonic conference, the Examiner tentatively agreed that inserting a "*method*" in Claim 23 would overcame the § 101 rejection. Applicant respectfully submits that Claim 23 is no longer directed to non-statutory subject matter and respectfully requests that the § 101 rejection be withdrawn.

Dependent Claims 24-29 depend directly or indirectly from independent Claim 23 and thus are allowable as depending from an allowable base claim. Applicant

respectfully submits that Claims 24-29 are no longer directed to non-statutory subject matter and respectfully requests that the § 101 rejections of these claims be withdrawn.

Claim Rejections Under 35 U.S.C. § 102(b)

Claims 1-5, 7, 9-13, 16-21, 23-28, and 30-33 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Application Publication No. 2001/0020228 A1 to Cantu et al. (hereinafter "Cantu"). Cantu incorporates the Handbook of Applied Cryptography (hereinafter "Handbook").

Applicant respectfully traverses the rejection.

Independent Claim 1

Without conceding the propriety of the stated rejections, and only to advance the prosecution of this application, Applicant amends independent Claim 1 to further clarify features of the subject matter. **Independent claim 1** as amended now recites an out-of-band method for asynchronously establishing a secure association with a server node, the method comprising:

> allowing a client node to remotely load an operating system;
> loading the operating system on the client node, wherein a profile of the operating system is stored on the server node;
> generating a local public value and a local private value on the client node;
> storing the public value for configuration of the secure association on an out-of band computer-readable storage medium, wherein the stored public value is not used for authentication;
> transporting the out-of-band computer-readable storage medium to the server node to establish a trust relationship allowing for remotely loading the operating system on the client node from the server node, wherein a low level of trust is required;
> receiving the public value from the server node via the out-of-band computer-readable storage medium; and

generating a secret value using the local private value in combination with the public value received from the server node; wherein the receiving is asynchronous to the generating.

Applicant respectfully submits that no such method is anticipated by Cantu. Specifically, Cantu fails to disclose remotely loading an operating system on the client node from the server node where a low level of trust is required between the nodes to establish a secure association, as recited in Applicant's amended Claim 1.

Cantu Fails to Disclose Remotely Loading an Operating System on the Client Node from the Server Node where a Low Level of Trust is Required Between the Nodes to Establish a Secure Association

Cantu is directed towards using relationships among entities to exchange encryption keys for use in providing access and authorization to resources (Cantu, para. 0003). In Cantu, each entity has one relationship with one other entity and uses preexisting relationships among entities to exchange the encrypting keys, assuring the entities as to the authenticity of the keys with a degree of certainty corresponding to the nature of the relationship (Cantu, paras. 0015, 0019, 0085). Cantu shows a transaction of a key occurring as a part of preexisting relationship where the key is sent through some secure channel, such as providing a computer diskette or through an encrypted e-mail message (Cantu, para. 0089).

Applicant's amended Claim 1 recites, in part, "*allowing a client node to remotely load an operating system; loading the operating system on the client node, wherein a profile of the operating system is stored on the server node*" and "*transporting the out-of-band computer-readable storage medium to the server node to establish a trust*

relationship allowing for remotely loading the operating system on the client node from the server node, wherein a low level of trust is required".

Contrary to Cantu, Applicant's amended Claim 1 shows establishing a trust relationship to provide for a secure association allowing a client node to remotely load an operating system from a server node (Application, pgs. 4-5, 7-9). Furthermore, Cantu does not show a secure association where merely a low level of trust is required, as recited in Applicant's amended Claim 1. Rather, Cantu shows that public keys can be safely exchanged because of preexisting relationships between the nodes, implying that without a preexisting relationship there could not be a secure association (*see* Cantu, para. 0019; in para. 0107). While Cantu briefly mentions "alternative secure techniques" that may or may not be a part of a transaction related to an preexisting relationship, there is no further discussion to define or support this statement. It follows that Cantu does not show establishing a secure association permitting a client node to remotely load an operating system from a server node where the trust relationship between the nodes requires only a low level of trust, as recited in Applicant's amended Claim 1.

Thus, Cantu fails to anticipate each and every element or feature of Applicant's amended Claim 1. Specifically, Cantu fails to disclose "*loading the operating system on the client node, wherein a profile of the operating system is stored on the server node*" and "*transporting the out-of-band computer-readable storage medium to the server node to establish a trust relationship allowing for remotely loading the operating system on the client node from the server node, wherein a low level of trust is required*", as recited in Applicant's amended Claim 1. Accordingly, Applicant respectfully requests that the § 102 rejection be withdrawn.

Independent Claims 9, 16, 23, and 30

Independent Claims 9, 16, 23, and 30 are directed to a computer-readable storage media, an apparatus, a method, and an apparatus, respectively, and each is allowable for reasons similar to those discussed above with respect to Claim 1.

Independent Claim 9 recites a computer-readable storage medium having one or more instructions causing one or more processors to:

> load an operating system on a processor, wherein a profile of the operating system is stored on an another processor;
>
> generate a local two-part code having a public code component and a private code component to allow the processor to remotely load the operating system from the another processor;
>
> store the public component on a peripheral out-of-band device which is then transported over an out-of-band mechanism to the another processor for configuration of a secure association and not authentication, wherein a low level of trust is required for transport;
>
> receive the public code component asynchronously from another processor via the peripheral device; and
>
> generate a secret value using the local private code component and the public code component received from the other processor.

Applicant respectfully submits that Cantu fails to anticipate these features as recited in Claim 9.

Independent Claim 16 recites an apparatus, comprising:

> a computer-readable storage medium;
>
> a key generator on a first node to generate a local public/private key pair;
>
> a computer processor executing code to write the local public/private key pair to an out-of-band computer-readable storage medium to facilitate setup of a secure association and not for authentication, wherein the secure association allows the first node to remotely load an operating system having a profile stored on a second node;
>
> a shared secret generator on the second node to receive the public key from the first node via the out-of-band computer-readable storage

medium connection without requiring a high degree of trust between the first node and the second node; and

the shared secret generator to generate a shared secret using the local private key and the public key received from the first node.

Applicant respectfully submits that Cantu fails to anticipate these features as recited in Claim 16.

Independent Claim 23 recites a method for running a protocol for establishing a trust relationship between two or more processing nodes, comprising:

generating a public key and a private key on each of at least two nodes allowing a first node of at least two nodes to remotely load an operating system, wherein a profile of the operating system is stored on a second node of at least two nodes;

exchanging the public keys asynchronously between the at least two nodes using an out-of-band mechanism comprising a computer-readable storage medium wherein the public keys are not used for authentication and without requiring a high degree of trust for an exchange of the public keys between the two nodes; and

calculating a secret to be shared on at least one of the two nodes.

Applicant respectfully submits that Cantu fails to anticipate these features as recited in Claim 23.

Independent Claim 30 recites an apparatus, comprising:

means for generating a local public/private key pair to allow a node to remotely load an operating system through a secure association with another node, wherein a profile of the operating system is stored on the another node;

means for storing a public key on an out-of-band computer-readable storage medium;

means for transporting asynchronously the public key to another node;

means for receiving at another node the public key from the out-of-band computer-readable storage medium wherein the public key is used for configuration of the secure association and not used for authentication; and

means for generating a shared secret using the local private key and the public key received from the other node asynchronously via the out-of-band computer-readable storage medium.

Applicant respectfully submits that Cantu fails to anticipate these features as recited in Claim 30.

Dependent Claims 2-5, 7, 10-13, 4, and 16-20 depend directly or indirectly from one of independent Claims 1, 8, and 15, respectively, and are allowable by virtue of this dependency. These claims are also allowable for their own recited features that, in combination with those recited in independent Claims 1, 8, and 15, are not anticipated by Cantu. For all of these reasons, Applicant respectfully request the §102(b) rejection of these claims be withdrawn.

Claim Rejections Under 35 U.S.C. § 103(a)

Claims 8, 15, 22, 29, and 34 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Cantu, in further view of Official Notice. Applicant respectfully traverses the rejection.

As explained above with respect to the rejections under § 102(b), Applicant submits that Cantu fails to disclose the features of independent Claims 1, 9, 16, 23, and 30. **Dependent Claims 8, 15, 22, 29, and 34** depend directly or indirectly from one of independent Claims 1, 9, 16, 23, and 30, respectively, and are allowable by virtue of this dependency. These claims are also allowable for their own recited features that, in combination with those recited in Claims 1, 9, 16, 23, and 30 are not disclosed, taught, or suggested by Cantu or Official Notice, alone or in combination.

Applicant respectfully submits that Cantu or Official Notice, alone or in combination, do not render the claimed subject matter obvious and that the claimed subject matter, therefore, is patentably distinguishable over the cited references. For all

of these reasons, Applicant respectfully request the §103(a) rejection of these claims be withdrawn.

CONCLUSION

Claims 1-5, 7-13, and 15-34 are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of the subject application. If any issue remains unresolved that would prevent allowance of this case, the Office is requested to contact the undersigned attorney to resolve the issue.

Respectfully submitted,

Lee & Hayes, PLLC

Dated: 12/04/2008

By: / Dino Kujundzic /
Dino Kujundzic
Reg. No. 63,104
509-944-4762

Shirley L. Anderson
Reg. No. 57,763
509-944-4758